UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,813	08/01/2003	Xiaomang Zhang	.24500-000006/US	2019

30593   7590   09/26/2007
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER
WANG, HARRIS C

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/631,813	ZHANG ET AL.
Office Action Summary	Examiner	Art Unit	
	Harris C. Wang	2139	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _01 August 2003_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-28_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-28_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

    1.☒ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _10/31/2005_.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1. Claims 1-28

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2, 6, 16, 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Claims recite the limitation "response request ID." The term "response request ID" is not well known in the art. It is unclear whether it is a response, a request or an ID that the Applicant is claiming.

Claims 3, 9-10, 17, 23-24 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 3, 9-10, 17, 23-24 recite the limitation "card company ID number." It is unclear what a "card company ID number." If it is a number of a "card company," the definition of "card company" is unclear. A card company can be broadly interpreted as a credit card company, a IC card manufacturing company, a playing card company and so on.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 4-7, 11-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Azuma (6704608).

Regarding Claims 1, 4-7, 11-14,

Azuma (6704608) teaches an authentication system comprising:

an IC card, and an electronic seal, wherein: the IC card includes:

a random number generation section for generating a random number, a prescribed key memory section for storing a prescribed key, a first encryption section for encrypting the generated random number based on the prescribed key, and a first output section for outputting the random number encrypted based on the prescribed key; ("The IC card generates a random number M, encrypts it using the public key Mb, and sends an encrypted numeral WM to the second terminal apparatus" Column 19, lines 66-67, Column 20, line 1) The Examiner interprets the prescribed key as a public key. The Examiner interprets that the public key must be inherently stored in a memory section before encrypting the random number with the public key. The Examiner interprets the output section as the section that outputs the encrypted random number to the second terminal device.

Azuma further teaches an electronic seal which includes:

a second input section for inputting the random number encrypted based on the prescribed key, a secret key memory section for storing a secret key related to the prescribed key, a second decoding section for decoding, based on the secret key, the random number encrypted based on the prescribed key, a second encryption section for encrypting, based on the secret key, the random number decoded based on the secret key, and a second output section for outputting the random number encrypted based on the secret key; *("The second terminal apparatus decrypts the numeral WM, using a secret key, encrypts it using a public key to obtain the numeral WN, and sends the numeral WN to the IC card." Column 20, lines 1-4) The Examiner interprets the secret key memory section, the section that stores the secret key used to encrypt the numeral WM. The Examiner interprets the second encrypting section as the section that encrypts based on the secret key. The Examiner interprets the second output section the section that sends the random number back to the IC card.*

Azuma further teaches the IC card further includes:

a first input section for inputting the random number encrypted based on the secret key, a first decoding section for decoding, based on the prescribed key, the random number encrypted based on the secret key, and a comparison section for comparing the random number generated by the random number generation section and the random number decoded based on the prescribed key; and the IC card and the electronic seal mutually exchange data for performing authentication. *("The IC card receives from the second terminal apparatus the numeral WN, obtains a numeral N by decrypting the numeral WN, and judges whether the numeral n matches the numeral M. When they do not match, the IC card abnormally ends the mutual authentication process. When they*

match, the IC card sends a confirmation command to the second terminal apparatus in step

S82 that ends the mutual authentication" Column 20, lines 5-11)

The Examiner interprets the first input section as the section that receives the random

number from the terminal. The Examiner interprets the first decoding section as the section

that decrypts the numeral WN. The Examiner interprets the comparison section as the judging

unit that judges whether the numeral n matches the numeral M.

Azuma teaches a mobile device including an electronic seal.

("the second terminal apparatus is used in a machine for payment, such as a cash dispenser"

Column 17, lines 5-6)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

Claims 2, 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Azuma.

Regarding Claim 2, 8 (103)

Azuma teaches an electronic seal according to claim 1, wherein:

when the input section inputs a first response request ID *("The second terminal*

apparatus is used in a machine for payment...a touch panel for receiving an input of an

identification number of an IC card owner" Column 17, lines 5-6, 11-12)

the electronic seal further includes a response request ID memory

section for storing a second response request ID, and a comparison section for

comparing the decoded first response request ID and the second response request

ID, *("The host apparatus has a database which stores a plurality of entries of IC card code*

numbers in correspondence with a plurality of pieces of bio-information, so that the host

apparatus can judge whether the card owner is proper" Column 18, lines 60-64)

and when the decoded first response request ID matches the second response

request ID, the encryption section encrypts the decoded random number ("When a

combination of the bio-information read by the sensor and the typed code number is

found in the database, the controller 73 goes to the process in the flowchart shown in

Figure 24" Column 19, lines 2-5)

Azuma does not explicitly teach the first response request ID encrypted by the IC

card based on the prescribed key, the output section of the IC card outputs the

encrypted response request ID to the electronic seal, and the decoding section of the electronic seal decodes the input first response request ID based on the secret key.

. While Azuma teaches encrypting and decrypting a random value, Azuma sends the ID without encryption. However because encrypting a random number is analogous with encrypting an ID and the IC already possess all the features described in order to encrypt and decrypt an ID with a secret key (encryptor, decryptor, secret key), without any modification to the system one of ordinary skill could encrypt the ID sent by the IC card with a public key, and the terminal would subsequently decrypt the ID with the secret key.

It would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the ID sent by the IC card described in Azuma with a secret key, and decode the ID based on the same secret key.

The motivation is that encrypting the ID would provide another level of security.

Claims 3, 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Azuma in view of Reece (20030150915).

Regarding Claim 3,

Azuma teaches an electronic seal according to claim 1, wherein: the secret key memory section stores a plurality of secret keys.

Azuma does not explicitly teach that the secret keys respectively corresponding to a plurality of card company ID numbers, and when the input section inputs a card company ID number, the secret key memory section specifies the secret key corresponding to the input card company ID number among the plurality of secret keys.

Reece (20030150915) teaches a smart card that contains a Card Holder Data unit (Figure 1, 1320) which in turn contains Card Holder company ID number. *("CH company ID number, Paragraph [0278]).*

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify assigning a secret key per each IC card as taught by Azuma with assigning a secret key corresponding to input card company ID number.

The motivation is that Reece teaches that company ID number is a well known way to represent and identify the Card Holder Data Unit. One of ordinary skill would have been able to modify the system of Azuma to correspond a plurality of secret keys with corresponding card company ID numbers.

Regarding Claim 9,

Azuma teaches an IC card according to claim 6. Azuma does not explicitly teach further comprising a card company ID number memory section for storing a card company ID number, wherein the output section outputs the card company ID number.

Reece (20030150915) teaches a smart card that contains a Card Holder Data

unit (Figure 1, 1320) which in turn contains Card Holder company ID number. *("CH*

company ID number, Paragraph [0278]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the IC card to comprise a card company ID number memory

section for storing a card company ID number.

The motivation is that Reece teaches that storing a company ID number is well

known for IC cards.

Regarding Claim 10,

Azuma teaches an IC card according to claim 6. Azuma does not explicitly teach

wherein the prescribed key memory section stores a plurality of prescribed keys

respectively corresponding to a plurality of card company ID numbers.

Reece (20030150915) teaches a smart card that contains a Card Holder Data

unit (Figure 1, 1320) which in turn contains Card Holder company ID number. *("CH*

company ID number, Paragraph [0278]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify assigning a secret key per each IC card as taught by Azuma with

assigning a secret key corresponding to input card company ID number.

The motivation is that Reece teaches that company ID number is a well known

way to represent and identify the Card Holder Data Unit. One of ordinary skill would

have been able to modify the system of Azuma to correspond a plurality of secret keys

with corresponding card company ID numbers.

Claims 15, 18-19, 20-21, 24, 25-27 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Azuma in view of Yu (6067621).

Regarding Claims 15-16, 18-19, 20-22, 24, 25-27,

Azuma (6704608) teaches an authentication system comprising:

an IC card, and an electronic seal, wherein: the IC card includes:

a random number generation section for generating a random number,

a prescribed key memory section for storing a prescribed key,

a first encryption section for encrypting the generated random number based on

the prescribed key,

and a first output section for outputting the random number encrypted based on

the prescribed key; ("*The IC card generates a random number M, encrypts it using the public

key Mb, and sends an encrypted numeral WM to the second terminal apparatus*" Column 19,

lines 66-67, Column 20, line 1) The Examiner interprets the prescribed key as a public key.

The Examiner interprets that the public key must be inherently stored in a memory section

before encrypting the random number with the public key. The Examiner interprets the output

section as the section that outputs the encrypted random number to the second terminal

device.

A first user's inherent information memory section for storing a user's inherent information. *("a second reading unit operable to read, after the portable card is inserted into the box, bio-information indicating physical characteristics of the owner, form the owner, and the communicating unit sets the integrated device to the second mode after confirming the authenticity of the owner or the portable card using one of the physically recorded information, the owner information, and the bio-information" Column 7, lines 4-11)*

the electronic seal includes:

a second input section for inputting the random number encrypted based on the prescribed key,

a secret key memory section for storing a secret key related to the prescribed key,

a second decoding section for decoding, based on the secret key, the random number encrypted based on the prescribed key,

a second encryption section for encrypting, based on the secret key, the random number decoded based on the secret key,

and a second output section for outputting the random number encrypted based on the secret key; *("The second terminal apparatus decrypts the numeral WM, using a secret key, encrypts it using a public key to obtain the numeral WN, and sends the numeral WN to the IC card." Column 20, lines 1-4) The Examiner interprets the secret key memory section, the section that stores the secret key used to encrypt the numeral WM. The Examiner interprets the second encrypting section as the section that encrypts based on the secret key. The Examiner interprets the second output section the section that sends the random number back to the IC card.*

a second user's inherent information section for storing user's inherent

information *("a bio-sensor for reading bio-information of the IC card owner, such as a face*

outline, irises in the eyes, or fingerprints" Column 17, lines 13-15)

the IC card further includes:

a first input section for inputting the random number encrypted based on the

secret key,

a first decoding section for decoding, based on the prescribed key, the random

number encrypted based on the secret key,

and a comparison section for comparing the random number generated by the

random number generation section and the random number decoded based on the

prescribed key; and the IC card and the electronic seal mutually exchange data for

performing authentication. *("The IC card receives from the second terminal apparatus the*

numeral WN, obtains a numeral N by decrypting the numeral WN, and judges whether the

numeral n matches the numeral M. When they do not match, the IC card abnormally ends the

mutual authentication process. When they match, the IC card sends a confirmation command

to the second terminal apparatus in step S82 that ends the mutual authentication" Column 20,

lines 5-11)

The Examiner interprets the first input section as the section that receives the random

number from the terminal. The Examiner interprets the first decoding section as the section

that decrypts the numeral WN. The Examiner interprets the comparison section as the judging

unit that judges whether the numeral n matches the numeral M.

Azuma teaches a mobile device including an electronic seal.

("the second terminal apparatus is used in a machine for payment, such as a cash dispenser"
Column 17, lines 5-6)

Azuma does not explicitly teach performing a one way hash function on the value output from the symmetrical key cipher algorithm, changing the random number into a predetermined value and storing it in the terminal...The one-time password is verified then by receiving the one-time password generated from the terminal, through a predetermined communication medium, reading the secret key and the random . number stored in the server, performing a symmetrical key cipher algorithm using the secret key and the random number as an input, performing a one way hash function on the valve output from the symmetrical key algorithm and authenticating a user, if the · predetermined format is the same as the received one time password, and not authenticating the user if not the same

Yu teaches a first hash operation section for performing a hash operation using an IC card's secret key and a random number as an input, *"performing a one way hash function on the value output from the symmetrical key cipher algorithm, changing the random number into a predetermined value and storing it in the terminal...The one-time password is verified then by receiving the one-time password generated from the terminal, through a predetermined communication medium, reading the secret key and the random number stored in the server, performing a symmetrical key cipher algorithm using the secret key and the random number as an input, performing a one way hash function on the valve output from the symmetrical key algorithm...and authenticating a user, if the predetermined format is the same as the received one time password, and not authenticating the user if not the same."* (Column 4, lines 44-65)

Azuma already teaches encryption with public/private keys. Hashing is a well known method of encryption.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Azuma to include a hash function, to generate a one-time password using a hash function to hash an input random number and secret key for the purpose of authentication.

The motivation is that Yu teaches a well known way of authenticating using a hash function, a secret key of an IC card and a random number.

Azuma and Yu do not teach not explicitly teach a first hash operation section for performing a hash operation using the user's inherent information stored in the first user's inherent information memory section and the generated random number so as to output a first hash operation result, a second hash operation section for performing a hash operation using the user's inherent information stored in the second user's inherent memory section and the decoded random number so as to output a second hash operation result, or a comparison section for comparing the first hash operation result and the decoded second has operation result.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Yu to instead hash a user's inherent information and random number instead of a secret key and a random number.

The motivation is that the system of Azuma already teaches inherent information, and one of ordinary skill in the art would be able to use the inherent information instead of a secret key when generating the hash.

Regarding Claims 16, 22

Azuma and Yu teach an electronic seal according to claim 15, wherein Azuma teaches:

when the input section inputs a first response request ID *("The second terminal*

apparatus is used in a machine for payment...a touch panel for receiving an input of an

identification number of an IC card owner" Column 17, lines 5-6, 11-12)

the electronic seal further includes a response request ID memory

section for storing a second response request ID, and a comparison section for

comparing the decoded first response request ID and the second response request

ID, *("The host apparatus has a database which stores a plurality of entries of IC card code*

numbers in correspondence with a plurality of pieces of bio-information, so that the host

apparatus can judge whether the card owner is proper" Column 18, lines 60-64)

and when the decoded first response request ID matches the second response

request ID, the encryption section encrypts the decoded random number ("When a

combination of the bio-information read by the sensor and the typed code number is

found in the database, the controller 73 goes to the process in the flowchart shown in

Figure 24" Column 19, lines 2-5)

Azuma and Yu do not explicitly teach the first response request ID encrypted by

the IC card based on the prescribed key, the output section of the IC card outputs the

encrypted response request ID to the electronic seal, and the decoding section of the

electronic seal decodes the input first response request ID based on the secret key.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to encrypt the ID sent by the IC card described in Azuma with a secret key,

and decode the ID based on the same secret key.

The motivation is that in the limitations described in Claim 1, the electronic seal

and the IC already possess all the features described in order to encrypt and decrypt an

ID with a secret key (encryptor, decryptor, secret key). However instead of encrypting

and decrypting a random value, instead an ID is encrypted and decrypted. Without any

modification to the system one of ordinary skill could encrypt the ID sent by the IC card

with a public key, and the terminal would subsequently decrypt the ID with the secret

key.

Claims 17, 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Azuma in view of Yu as applied to claim15 above, and further in view of Reece.

Regarding Claim 17,

Azuma and Yu teach an electronic seal according to claim 15, wherein Azuma teaches:

the secret key memory section stores a plurality of secret keys.

Azuma does not explicitly teach that the secret keys respectively corresponding

to a plurality of card company ID numbers, and when the input section inputs a card

company ID number, the secret key memory section specifies the secret key

corresponding to the input card company ID number among the plurality of secret

keys.

Reece (20030150915) teaches a smart card that contains a Card Holder Data

unit (Figure 1, 1320) which in turn contains Card Holder company ID number. *("CH*

company ID number, Paragraph [0278]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify assigning a secret key per each IC card as taught by Azuma with

assigning a secret key corresponding to input card company ID number.

The motivation is that Reece teaches that company ID number is a well known

way to represent and identify the Card Holder Data Unit. One of ordinary skill would

have been able to modify the system of Azuma to correspond a plurality of secret keys

with corresponding card company ID numbers.

Regarding Claim 23,

Azuma and Yu teach an IC card according to claim 20. Azuma does not explicitly

teach further comprising a card company ID number memory section for storing a card

company ID number, wherein the output section outputs the card company ID number.

Reece (20030150915) teaches a smart card that contains a Card Holder Data

unit (Figure 1, 1320) which in turn contains Card Holder company ID number. *("CH*

company ID number, Paragraph [0278]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the IC card to comprise a card company ID number memory section for storing a card company ID number.

The motivation is that Reece teaches that storing a company ID number is well known for IC cards.

Regarding Claim 24,

Azuma and Yu teach an IC card according to claim 20. Azuma does not explicitly teach wherein the prescribed key memory section stores a plurality of prescribed keys respectively corresponding to a plurality of card company ID numbers.

Reece (20030150915) teaches a smart card that contains a Card Holder Data unit (Figure 1, 1320) which in turn contains Card Holder company ID number. ("CH company ID number, Paragraph [0278]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify assigning a secret key per each IC card as taught by Azuma with assigning a secret key corresponding to input card company ID number.

The motivation is that Reece teaches that company ID number is a well known way to represent and identify the Card Holder Data Unit. One of ordinary skill would have been able to modify the system of Azuma to correspond a plurality of secret keys with corresponding card company ID numbers.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

SYED A. ZIA
PRIMARY EXAMINER